RECEIVED
CENTRAL FAX CENTER
JUN 0 2 2008

US 09/747,511

PROPOSED AMENDED CLAIMS

1-59 (Cancelled)

60. (Currently Amended) A method of electronically negotiating an electronic negotiable document in the form of an electronic bank cheque having a monetary value and sold by a seller to a buyer, wherein said seller is not a bank, the method comprising:

providing said seller with seller tamper-resistant document carrier hardware, said seller tamper-resistant document carrier hardware having its own public-secret key pair, and wherein said secret key is not accessible to said seller, said document carrier bearing said electronic negotiable document and a signature calculated using said secret key;

providing said buyer with buyer tamper-resistant document carrier hardware, said buyer tamper-resistant document carrier hardware having its own public-secret key pair, and wherein said secret key is not accessible to said buyer;

transferring said electronic negotiable document from said seller tamper-resistant document carrier hardware to said buyer tamper-resistant document carrier hardware;

splitting said electronic ~~negotiable document~~ bank cheque electronically in said buyer tamper-resistant document carrier hardware into two or more split versions of said ~~new~~ electronic ~~negotiable document~~ bank cheque with each split version comprising the original electronic bank cheque, a sequence number and having a monetary value such that the sum of the monetary values of said two or more split versions ~~new electronic negotiable document~~ adds up to said monetary value of said electronic ~~negotiable document~~ bank cheque;

digitally signing said ~~splitting~~ said split versions using said secret key of said buyer tamper-resistant document carrier hardware to generate a splitting signature; and, without settlement of an account with a said bank,

negotiating said two or more split versions ~~new electronic negotiable documents~~ separately to one or more further buyers without the involvement of a trusted third party (TTP);

wherein said digitally signing of ~~splitting~~ said split versions comprises subjecting each of said two or more said split versions ~~new electronic negotiable document~~ to said secret key of said buyer tamper-resistant document carrier hardware; and

wherein said electronic ~~negotiable document~~ bank cheque ~~and said two or more new electronic negotiable documents each have~~ has an associated sequence number, and wherein said electronic ~~negotiable document~~ bank cheque, including its said associated sequence number, is signed by said secret key of the seller tamper-resistant document carrier hardware~~, and wherein each of said new electronic negotiable documents, each including its said associated sequence number, is signed by said secret key of the buyer tamper-resistant document carrier hardware~~.

61-62 (Canceled)

63. (Currently amended) The method as claimed in claim ~~62~~ 61 wherein said seller and said buyer tamper-resistant document carrier hardware each have a document carrier identifier, and wherein each said document carrier identifier is signed by a said secret key.

64. (Previously presented) The method as claimed in claim 60 wherein said seller tamper-resistant document carrier hardware bears an issuing signature, and wherein said transferring includes transferring said issuing signature from said seller tamper-resistant document carrier hardware to said buyer tamper-resistant document carrier hardware.

65. (Previously presented) The method as claimed in claim 64 further comprising deleting said issuing signature after said transferring.

66. (Cancelled).

67. (new) A method of electronically negotiating an electronic negotiable document in the form of an electronic bill of lading having a monetary value and sold by a seller to a buyer, wherein said seller is not a bank, the method comprising:

providing said seller with seller tamper-resistant document carrier hardware, said seller tamper-resistant document carrier hardware having its own public-secret key pair, and wherein said secret key is not accessible to said seller, said document carrier bearing said electronic negotiable document and a signature calculated using said secret key;

providing said buyer with buyer tamper-resistant document carrier hardware, said buyer tamper-resistant document carrier hardware having its own public-secret key pair, and wherein said secret key is not accessible to said buyer;

transferring said electronic negotiable document from said seller tamper-resistant document carrier hardware to said buyer tamper-resistant document carrier hardware;

splitting said electronic bill of lading electronically in said buyer tamper-resistant document carrier hardware into two or more split versions of said electronic bill of lading with each split version comprising the original electronic bill of lading, a sequence number and having a monetary value such that the sum of the monetary values of said two or more split versions adds up to said monetary value of said electronic bill of lading;

digitally signing said split versions using said secret key of said buyer tamper-resistant document carrier hardware to generate a splitting signature; and, without settlement of an account with a said bank,

negotiating said two or more split versions separately to one or more further buyers without the involvement of a trusted third party (TTP);

wherein said digitally signing of said split versions comprises subjecting each of said two or more said split versions to said secret key of said buyer tamper-resistant document carrier hardware; and

wherein said electronic bill of lading has an associated sequence number, and wherein said electronic bill of lading, including its said associated sequence number, is signed by said secret key of the seller tamper-resistant document carrier hardware.

68. (new) A method of electronically negotiating an electronic negotiable document in the form of an electronic bill of lading having a quantity of goods and sold by a seller to a buyer, wherein said seller is not a bank, the method comprising:

providing said seller with seller tamper-resistant document carrier hardware, said seller tamper-resistant document carrier hardware having its own public-secret key pair, and wherein said secret key is not accessible to said seller, said document carrier bearing said electronic negotiable document and a signature calculated using said secret key;

providing said buyer with buyer tamper-resistant document carrier hardware, said buyer tamper-resistant document carrier hardware having its own public-secret key pair, and wherein said secret key is not accessible to said buyer;

transferring said electronic negotiable document from said seller tamper-resistant document carrier hardware to said buyer tamper-resistant document carrier hardware;

splitting said electronic bill of lading electronically in said buyer tamper-resistant document carrier hardware into two or more split versions of said electronic bill of lading with each split version comprising the original electronic bill of lading, a sequence number and having a quantity of goods such that the sum of the quantity of goods of said two or more split versions adds up to said quantity of goods of said electronic bill of lading;

digitally signing said split versions using said secret key of said buyer tamper-resistant document carrier hardware to generate a splitting signature; and, without settlement of an account with a said bank,

negotiating said two or more split versions separately to one or more further buyers without the involvement of a trusted third party (TTP);

wherein said digitally signing of said split versions comprises subjecting each of said two or more said split versions to said secret key of said buyer tamper-resistant document carrier hardware; and

wherein said electronic bill of lading has an associated sequence number, and wherein said electronic bill of lading, including its said associated sequence number, is signed by said secret key of the seller tamper-resistant document carrier hardware.

RECEIVED
CENTRAL FAX CENTER
JUN 0 2 2008

US 09/747,511

PROPOSED AMENDED CLAIMS

1-59 (Cancelled)

60. (Currently Amended) A method of electronically negotiating an electronic negotiable document in the form of an electronic bank cheque having a monetary value and sold by a seller to a buyer, wherein said seller is not a bank, the method comprising:

providing said seller with seller tamper-resistant document carrier hardware, said seller tamper-resistant document carrier hardware having its own public-secret key pair, and wherein said secret key is not accessible to said seller, said document carrier bearing said electronic negotiable document and a signature calculated using said secret key;

providing said buyer with buyer tamper-resistant document carrier hardware, said buyer tamper-resistant document carrier hardware having its own public-secret key pair, and wherein said secret key is not accessible to said buyer;

transferring said electronic negotiable document from said seller tamper-resistant document carrier hardware to said buyer tamper-resistant document carrier hardware;

splitting said electronic ~~negotiable document~~ bank cheque electronically in said buyer tamper-resistant document carrier hardware into two or more split versions of said ~~new~~ electronic ~~negotiable document~~ bank cheque with each split version comprising the original electronic bank cheque, a sequence number and having a monetary value such that the sum of the monetary values of said two or more split versions ~~new electronic negotiable document~~ adds up to said monetary value of said electronic ~~negotiable document~~ bank cheque;

digitally signing said ~~splitting~~ said split versions using said secret key of said buyer tamper-resistant document carrier hardware to generate a splitting signature; and, without settlement of an account with a said bank,

negotiating said two or more split versions ~~new electronic negotiable documents~~ separately to one or more further buyers without the involvement of a trusted third party (TTP);

wherein said digitally signing of ~~splitting~~ said split versions comprises subjecting each of said two or more said split versions ~~new electronic negotiable document~~ to said secret key of said buyer tamper-resistant document carrier hardware; and

wherein said electronic ~~negotiable document~~ bank cheque ~~and said two or more new electronic negotiable documents each have~~ has an associated sequence number, and wherein said electronic ~~negotiable document~~ bank cheque, including its said associated sequence number, is signed by said secret key of the seller tamper-resistant document carrier hardware~~, and wherein each of said new electronic negotiable documents, each including its said associated sequence number, is signed by said secret key of the buyer tamper-resistant document carrier hardware~~.

61-62 (Canceled)

63. (Currently amended) The method as claimed in claim ~~62~~ 61 wherein said seller and said buyer tamper-resistant document carrier hardware each have a document carrier identifier, and wherein each said document carrier identifier is signed by a said secret key.

64. (Previously presented) The method as claimed in claim 60 wherein said seller tamper-resistant document carrier hardware bears an issuing signature, and wherein said transferring includes transferring said issuing signature from said seller tamper-resistant document carrier hardware to said buyer tamper-resistant document carrier hardware.

65. (Previously presented) The method as claimed in claim 64 further comprising deleting said issuing signature after said transferring.

66. (Cancelled).

67. (new) A method of electronically negotiating an electronic negotiable document in the form of an electronic bill of lading having a monetary value and sold by a seller to a buyer, wherein said seller is not a bank, the method comprising:

providing said seller with seller tamper-resistant document carrier hardware, said seller tamper-resistant document carrier hardware having its own public-secret key pair, and wherein said secret key is not accessible to said seller, said document carrier bearing said electronic negotiable document and a signature calculated using said secret key;

providing said buyer with buyer tamper-resistant document carrier hardware, said buyer tamper-resistant document carrier hardware having its own public-secret key pair, and wherein said secret key is not accessible to said buyer;

transferring said electronic negotiable document from said seller tamper-resistant document carrier hardware to said buyer tamper-resistant document carrier hardware;

splitting said electronic bill of lading electronically in said buyer tamper-resistant document carrier hardware into two or more split versions of said electronic bill of lading with each split version comprising the original electronic bill of lading, a sequence number and having a monetary value such that the sum of the monetary values of said two or more split versions adds up to said monetary value of said electronic bill of lading;

digitally signing said split versions using said secret key of said buyer tamper-resistant document carrier hardware to generate a splitting signature; and, without settlement of an account with a said bank,

negotiating said two or more split versions separately to one or more further buyers without the involvement of a trusted third party (TTP);

wherein said digitally signing of said split versions comprises subjecting each of said two or more said split versions to said secret key of said buyer tamper-resistant document carrier hardware; and

wherein said electronic bill of lading has an associated sequence number, and wherein said electronic bill of lading, including its said associated sequence number, is signed by said secret key of the seller tamper-resistant document carrier hardware.

68. (new) A method of electronically negotiating an electronic negotiable document in the form of an electronic bill of lading having a quantity of goods and sold by a seller to a buyer, wherein said seller is not a bank, the method comprising:

providing said seller with seller tamper-resistant document carrier hardware, said seller tamper-resistant document carrier hardware having its own public-secret key pair, and wherein said secret key is not accessible to said seller, said document carrier bearing said electronic negotiable document and a signature calculated using said secret key;

providing said buyer with buyer tamper-resistant document carrier hardware, said buyer tamper-resistant document carrier hardware having its own public-secret key pair, and wherein said secret key is not accessible to said buyer;

transferring said electronic negotiable document from said seller tamper-resistant document carrier hardware to said buyer tamper-resistant document carrier hardware;

splitting said electronic bill of lading electronically in said buyer tamper-resistant document carrier hardware into two or more split versions of said electronic bill of lading with each split version comprising the original electronic bill of lading, a sequence number and having a quantity of goods such that the sum of the quantity of goods of said two or more split versions adds up to said quantity of goods of said electronic bill of lading;

digitally signing said split versions using said secret key of said buyer tamper-resistant document carrier hardware to generate a splitting signature; and, without settlement of an account with a said bank,

negotiating said two or more split versions separately to one or more further buyers without the involvement of a trusted third party (TTP);

wherein said digitally signing of said split versions comprises subjecting each of said two or more said split versions to said secret key of said buyer tamper-resistant document carrier hardware; and

wherein said electronic bill of lading has an associated sequence number, and wherein said electronic bill of lading, including its said associated sequence number, is signed by said secret key of the seller tamper-resistant document carrier hardware.

US 11/708,267

Amendments to claims finally rejected in view of Pats. 5,606,609 (Houser) and 5,224,166 (Hartman Jr.) in parent Serial No. 09/747,511

~~25~~ 1. A method of electronically issuing an electronic negotiable document (END), the method comprising:

creating as data an END and storing this in tamper-resistant document carrier hardware, the document carrier hardware containing a unique public-secret key pair for signing and verifying, and a unique document-carrier identifier;

signing the unique document-carrier identifier, the END and an END identifier using the secret key of the public-secret key pair; and

storing a ~~the~~ result of said signing in ~~the~~ said tamper-resistant document-carrier hardware, such that said secret key is not accessible to an owner of said tamper-resistant document carrier hardware.

(new) 2. A method as claimed in claim 1 wherein said result of said signing comprises a digital signature, and wherein said digital signature is only accessible by other said tamper-resistant document carrier hardware, encrypted by a public key of said other tamper-resistant document carrier hardware.

(new) 3. A method as claimed in claim 2 wherein said encrypted digital signature is only accessible once.

~~26~~ 4. A method according to claim ~~25~~ 1 of issuing an END, further comprising generating a time stamp representing the time of issue and storing this with the END in the tamper-resistant document carrier hardware before the signing step, and

~~27 A method according to claim 25 of issuing an END~~ including the step of calculating a hash value of one or both of the END and~~/or~~ the time stamp value and storing this hash value instead of the full END in the tamper-resistant document carrier hardware, before the said signing step.

28-30 Cancelled

~~31~~ 5. A method according to claim ~~25~~ 1 of issuing an END, in which the document carrier hardware stores a negotiability status flag indicative of whether the END stored therein is negotiable or non-negotiable, and including the step of setting the flag to "negotiable" after the result of the encryption has been stored in the document carrier hardware.

~~32~~ 6. A method according to claim ~~25~~ 1 of issuing an END, in which the document carrier hardware includes a counter for counting a serial number, indicative of the number of times that the END has been negotiated since issue, and comprising the step of setting the counter to zero after the result of the encryption has been stored in the document carrier hardware.

~~33~~ 7. Tamper-resistant document carrier hardware adapted to store an END in accordance with the method of claim ~~25~~ 1, said hardware comprising read only software for controlling the steps of storing the END, encrypting the END and other data with said secret key, and storing the result in a memory.

34-35 Cancelled

~~36~~ 8. A method of electronically negotiating an END between a seller and a buyer, said seller and said buyer each possessing tamper-resistant document carrier hardware having its own public-secret key pair, the method comprising:

providing an ~~in which the~~ END ~~is~~ stored in ~~the seller's~~ tamper-resistant document carrier hardware of a seller in the form of END data ~~and the~~ with a signature generated by ~~the secret signing~~ a secret key of a document carrier of the issuer of the END ~~together~~, and with a negotiability status flag indicative of whether the END is currently negotiable from ~~the~~ said tamper-resistant document carrier hardware ~~on which it is stored~~ of said seller, said tamper-resistant document carrier hardware of said seller having its own public-secret key and being configured such that said secret key of said public-secret key pair is not accessible to said seller;

~~comprising~~ establishing mutual recognition between ~~the~~ said seller and a buyer using one or more predetermined protocols between ~~the buyer's and seller's~~ said tamper-resistant document carrier hardwares of said seller and tamper-resistant document carrier hardware of said buyer, said tamper-resistant document carrier

hardware of said buyer having its own public-secret key and being configured such that said secret key of said public-secret key pair is not accessible to said buyer;

verifying in ~~the seller's~~ said tamper-resistant document carrier hardware of said seller that said negotiability status flag is "negotiable" and aborting the negotiation if not;

sending ~~the~~ said public encryption key of ~~the buyer's~~ said tamper-resistant document carrier hardware of said buyer to ~~the seller's~~ said tamper-resistant document carrier hardware of said seller;

using ~~it~~ said public key of said tamper-resistant document carrier hardware of said buyer in said tamper-resistant document carrier hardware of said seller to encrypt a message comprising said signature, said END ~~together with~~ and said negotiability status flag;

sending ~~that~~ said encrypted message to ~~the buyer's~~ said tamper-resistant document carrier hardware of said buyer;

decrypting ~~that~~ said encrypted message in said tamper-resistant document carrier hardware of said buyer using ~~the buyer's~~ said secret ~~decryption~~ encryption key of said tamper-resistant document carrier hardware of said buyer; and

setting ~~the~~ a negotiability status flag for ~~that~~ said END ~~of the buyer's and seller's~~ in said tamper-resistant document carrier hardware of said buyer and said seller respectively to "negotiable" and "non-negotiable".

Claim 37 – see claim 12

~~38~~ 9. A method according to claim ~~36~~ 8 in which said tamper-resistant document carrier hardware ~~is installed originally with~~ of each of said buyer and said seller carries a digital certificate comprising a digital signature of ~~its~~ a unique identifier and of ~~its~~ said public key of said tamper-resistant document carrier hardware, the method further comprising

~~42 A method according to claim 38, in which the~~ sending said digital certificate of ~~the buyer's~~ said tamper-resistant document carrier hardware ~~is sent~~ of said buyer to ~~the seller's~~ said tamper-resistant document carrier hardware of said seller ~~in which it is authenticated~~, authenticating said digital certificate of said tamper-resistant document carrier hardware of said buyer, and aborting said ~~the~~ negotiation ~~is aborted~~ if said authenticating ~~authentication~~ fails.

Claim 39 cancelled

~~40~~ 10. A method according to claim ~~38~~ 9 in which a ~~the~~ digital certificate unique to ~~the~~ document carrier hardware on which ~~the~~ said END was originally issued is stored with ~~the~~ said END in ~~the seller's~~ said tamper-resistant document carrier hardware of said seller.

Claims 41 to 51 (except 37) – cancelled

11 (new). A method according to claim 8 further comprising, prior to said negotiating of said END, electronically issuing said END by:

creating as data an END and storing this in tamper-resistant document carrier hardware, the document carrier hardware containing a unique public-secret key pair for signing and verifying, and a unique document-carrier identifier;

signing the unique document-carrier identifier, the END and an END identifier using the secret key of the public-secret key pair; and

storing a result of said signing in said tamper-resistant document-carrier hardware, such that said secret key is not accessible to an owner of said tamper-resistant document carrier hardware.

~~52~~ 12. A method according to claim ~~36, including~~ 8 wherein said END has a predetermined period of validity, the method further comprising:

inhibiting recovery of a lost END until expiry of said predetermined period of validity of the END; and

after said expiry performing one or both of:

recovering ~~the~~ negotiation of an END which has previously broken down, by providing ~~the buyer's~~ said tamper-resistant document carrier hardware of said buyer with ~~the necessary~~ said secret key of said tamper-resistant document carrier hardware of said buyer which ~~has been~~ is not accessible to said buyer, reproduced by ~~the~~ an issuer of said secret key or by a trusted third party; and

~~54 A method according to claim 36, including~~ recovering an END lost from primary said tamper-resistant document carrier hardware, by activating back-up tamper-

resistant document carrier hardware which has previously been provided with back-up data reproduced from said primary tamper-resistant document carrier hardware.

~~37~~ 13. A method of electronically negotiating an END between a seller and a buyer, said seller and said buyer each possessing ~~a~~ tamper-resistant document carrier hardware having its own public-secret key pair, the method comprising:

providing an ~~in which the~~ END stored in ~~the seller's~~ said tamper-resistant document carrier hardware of a seller in the form of END data ~~and the~~ with a signature generated by ~~the~~ a secret signing-key of a document carrier ~~hardware~~ of the issuer of ~~the~~ said END ~~together~~, and with a serial number counter indicative of ~~the~~ a number of times that ~~the~~ said END has been negotiated since issue, said tamper-resistant document carrier hardware of said seller having its own public-secret key and being configured such that said secret key of said public-secret key pair is not accessible to said seller; ~~comprising~~

establishing mutual recognition between said seller and said buyer using one or more predetermined protocols between ~~the buyer's and seller's~~ said tamper-resistant document carrier hardware of said seller and tamper-resistant document carrier hardware of said buyer, said tamper-resistant document carrier hardware of said buyer having its own public-secret key and being configured such that said secret key of said public-secret key pair is not accessible to said buyer;

verifying in ~~the seller's~~ said tamper-resistant document carrier hardware of said seller that ~~the~~ said END, if it has been stored previously in ~~that~~ said tamper-resistant document carrier hardware of said seller, has a different counter value this time and is therefore negotiable;

sending ~~the~~ said public encryption key of ~~the buyer's~~ said tamper-resistant document carrier hardware of said buyer to ~~the seller's~~ said tamper-resistant document carrier hardware of said seller;

using ~~it~~ said public key of said tamper-resistant document carrier hardware of said buyer in said tamper-resistant document carrier hardware of said seller to encrypt a message comprising said signature, said END ~~together with the~~ and a value of said counter;

sending ~~that~~ said encrypted message to ~~the buyer's~~ said tamper-resistant document carrier hardware of said buyer;

decrypting ~~that~~ said encrypted message in said tamper-resistant document carrier hardware of said buyer using ~~the buyer's~~ said secret ~~decryption~~ encryption key of said tamper-resistant document carrier hardware of said buyer; and

incrementing said counter by one.

~~53~~ 14. A method according to claim ~~36, including~~ 12 wherein said END has a predetermined period of validity, the method further comprising:

inhibiting recovery of a lost END until expiry of said predetermined period of validity of the END; and

after said expiry performing one or both of:

recovering ~~the~~ negotiation of an END which has previously broken down, by providing ~~the buyer's~~ said tamper-resistant document carrier hardware of said buyer with ~~the necessary~~ said secret key of said tamper-resistant document carrier hardware of said buyer which ~~has been~~ is not accessible to said buyer, reproduced by ~~the~~ an issuer of said secret key or by a trusted third party; and

~~55 A method according to claim 37, including~~ recovering an END lost from primary said tamper-resistant document carrier hardware, by activating back-up tamper-resistant document carrier hardware which has previously been provided with back-up data reproduced from said primary tamper-resistant document carrier hardware.